IASSNS-HEP-95/15; quant-ph:9503005

Simple Realization Of The Fredkin Gate Using A Series Of Two-body Operators*

H. F. Chau and F. Wilczek
School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, U.S.A.

(February 1, 2008)

Abstract

The Fredkin three-bit gate is universal for computational logic, and is reversible. Classically, it is impossible to do universal computation using reversible two-bit gates only. Here we construct the Fredkin gate using a combination of six two-body reversible (quantum) operators.

PACS numbers: 03.65.Bz, 02.70.-c, 05.50.+q, 89.80.+h

* Accepted by *Phys. Rev. Lett.*

Since the pioneering work of Feynman and Deutsch [1,2], the potential to do universal computation in a closed system, using elements following the laws of quantum mechanics, has been recognized. There are also important problems for which it seems likely that quantum computers, if they can be realized, will have capabilities qualitatively superior to classical ones. The most obvious problems in this class, perhaps, involve simulation of the dynamics of quantum systems. Recently Shor [3] discovered a much less obvious application to a naturally defined problem: factorizing large numbers. His probabilistic algorithm for factorizing large composite numbers N using a quantum computer whose running time is polynomial in $\log N$, whereas all known classical algorithms are non-polynomial in this variable. Other relevant investigations include explorations of the possible physical implementation of quantum computers [4,5], quantum computational complexity classes [6], quantum teleportation [7], and quantum coding [8].

In the earliest work, the question of how a quantum mechanical computer, whose operation relies on (reversible) unitary matrices, can perform classical irreversible logical operations like AND was addressed. It was realized that reversibility can be maintained at the price of carrying around extra "garbage bits". Indeed, previous work on classical reversible computation had demonstrated that one could construct a universal machine using simple reversible three-in three-out prototypes. In particular the Fredkin gate [9] (see Fig. 1), whose characteristic is tabulated in Table I is known to be universal. For example, by fixing $c_i = 0$ in the input, it is easy to verify that c_o gives us the logical AND between a_i and b_i in the output. Other irreversible logical operations can be recovered in a similar manner. We represent 0 and 1 by $|0\rangle$ and $|1\rangle$ respectively. Then quantum mechanically, the Fredkin gate logic corresponds to the following three-body unitary transformation:

$$U_{\text{Fredkin}} = I + a^\dagger a \left(b^\dagger c + c^\dagger b - b^\dagger b - c^\dagger c + 2 b^\dagger b c^\dagger c \right), \tag{1}$$

where a and $a^\dagger$ denote the annihilation and creation operators at site a respectively. Since U_{Fredkin} is a three-body operator, its direct implementation would seem to require delicate cancellation of more fundamental two-body interactions, to leave behind a specific complicated three-body residual, which is very awkward.

Thus one is motivated to inquire whether U_{Fredkin} can be constructed using a (finite) composition of two-body operators. This question has been partially answered by DiVincenzo [11], who proposes a method to approximate Fredkin gate logic up to any accuracy $\epsilon > 0$ by $O(1/\sqrt{\epsilon})$ two-body unitary operators. Clearly, this result leaves room for improvement. DiVincenzo and Smolin [12] have done extensive numerical work, producing convincing evidence that any three-bit gate can be constructed by a suitable combination of six two-bit gates. In this note, we explicitly construct U_{Fredkin} using six two-body unitary operators. By way of contrast no combination of classical reversible two-bit gates is sufficient for universal computation, so that our construction provides another example of a qualitative enhancement of computational power through quantum mechanics.

Let us now introduce three basic gates used in our construction. A quantum-NOT gate is a one-in one-out quantum gate (see Fig. 2(a)), performing the unitary transformation

$$N_{(a)} |\alpha\rangle_a = \sigma_1 |\alpha\rangle_a, \tag{2}$$

where σ_i are the Pauli spin matrices, is an extension of the classical logical NOT to the quantum regime. We may also interpret the quantum-NOT gate as the one which gives

$(a+1)$ mod 2 from an input q-bit a. Diagrammatically, we represent a quantum-NOT gate as a rectangular box labeled by N (see Fig. 2(a)). Clearly, this is a one-body operator.

A conditional-U gate is a two-in two-out quantum logic gate (see Fig. 2(b)), performing the unitary transformation

$$U_{(a,b)}|\alpha\rangle_a|\beta\rangle_b = \left(1 - a^\dagger a\right)|\alpha\rangle_a|\beta\rangle_b + a^\dagger a|\alpha\rangle_a U|\beta\rangle_b. \tag{3}$$

Here, $|\alpha\rangle_a$ is used as a control, whose state will not change after passing through the gate. When $|\alpha\rangle_a = |0\rangle$, the gate does nothing. And when $|\alpha\rangle_a = |1\rangle$, state $|\beta\rangle_b$ is mapped to $U|\beta\rangle_b$. As shown in Fig. 2(b), we represent a conditional-U gate by a rectangular box labeled by U. The control q-bit (a in this case) is represented by drawing a dash line between the input (a_i) and the output (a_o). A conditional-U gate defines a two-body operator.

In particular, the conditional-σ_1 is of great importance. One can write down the "truth table" of this gate and find that it performs conditional NOT on the second q-bit b using the first q-bit a as control. In order to make the meaning of this gate more apparent, we denote this gate by conditional-N.

Finally, we introduce a doubly-controlled phase shifter (see Fig. 2(c)), which performs

$$P_{(a,b)}|\alpha\rangle_a|\beta\rangle_b = |\alpha\rangle_a|\beta\rangle_b - (1-P)a^\dagger a|\alpha\rangle_a b^\dagger b|\beta\rangle_b, \tag{4}$$

for some phase rotation $P = e^{i\theta}$. This is again a two-body operator, which changes the phase of the overall wavefunction provided that both a and b are in state $|1\rangle$, while q-bit c is entirely passive. We represent a doubly-controlled phase shifter as by a rectangular box labeled by P (see Fig. 2(c)).

We can now record our Fredkin gate construction. As shown in Fig. 3, it is a four stage construction consequentially making up of an adder, an $i\sigma_1$ generator, an i remover, and a subtracter. It corresponds to the following equation:

$$U_{\text{Fredkin}}(a,b,c) = N_{(c,b)} \circ N_{(c)} \circ P_{(a,b)} \circ U_{(a,c)} \circ V_{(b,c)} \circ U_{(a,c)} \circ V_{(b,c)} \circ N_{(c)} \circ N_{(c,b)}, \tag{5}$$

where $U = \sigma_2$, $V = (\sigma_2 + \sigma_3)/\sqrt{2}$, and $P = -i$. Since the first two of these operators act only on q-bits b and c, they can be combined; similarly the last three can be combined. Thus we have a six two-body gate realization as advertised.

Let us now explain how this construction works. First we want to gather all the quantum states that might be changed upon passing through a Fredkin gate to the third q-bit c. The most economical way to do this is by performing an addition modulo 4 in q-bits b and c. This can be done by a combination of a quantum-NOT and a conditional-U gates (see Fig. 3). After the core computation, we can of course reverse the above process using a subtracter. This accounts for a total of four gates. Using $|0,0,0\rangle$, $|0,0,1\rangle$, $\cdots$, $|1,1,1\rangle$ as our basis, and denoting them by 1, 2, $\cdots$, 8 respectively, then the combined action of the adder and the subtracter is to relabel the basis in the order of 4, 1, 2, 3, 8, 5, 6, and 7 . In the new representation, U_{Fredkin} becomes the matrix

$$U_{\text{Toffoli}} = \begin{bmatrix} I_6 & 0 \\ 0 & \sigma_1 \end{bmatrix}, \tag{6}$$

where I_6 is the 6×6 identity matrix. The U_{Toffoli} logic, which is sometimes called the Toffoli gate [10] or the "controlled controlled NOT gate" [2], is also known to be universal. The

convenient feature of the new basis is that the first two q-bits a and b are unaltered after the operation U_{Toffoli}. In addition, the third q-bit c changes its state when and only when a and b are both spin up.

Inspired by the idea of commutators in group theory, we ask if it is possible to construct two conditional-U gates such that

$$U_{(a,c)} \circ V_{(b,c)} \circ U^{-1}_{(a,c)} \circ V^{-1}_{(b,c)} = U_{\text{Toffoli}}. \tag{7}$$

This is possible when

$$UVU^{-1}V^{-1} = \sigma_1. \tag{8}$$

Unfortunately, Eq. (8) cannot be satisfied. A contradiction is arrived by taking the determinant in both sides of the equation. However, if we replace σ_1 by $i\sigma_1$ in Eq. (8), like what DiVincenzo has done in Ref [11], solutions can be found. One of the possible solutions is $U = \sigma_2$ and $V = (\sigma_2 + \sigma_3)/\sqrt{2}$. This solution has a nice feature that $U = U^{-1}$ and $V = V^{-1}$, which makes the actual construction of the machine a bit simpler. We call it the $i\sigma_1$ generator in Fig. 3, which eats up another four two-body gates. One can show that it is a minimal construction, in the sense that any proposal involving fewer than four two-bit gates cannot do the same computation. Alternative constructions of the Toffoli gate has been proposed by various authors [13].

Finally, we have to remove the extra phase i from the system. This can be done trivially by using a doubly-controlled phase shifter with $P = -i$ (see Fig 3). This completes our construction.

In summary, we have explicitly constructed a sequence of six two-body quantum gates to realize the three-in three-out Fredkin gate logic. As we have mentioned, this bypasses one significant barrier toward the possible construction of a quantum computer. Our construction can be used in the realization of other similar quantum gates as well. For example, the matrix

$$M = \begin{bmatrix} I_6 & 0 \\ 0 & \cos\lambda + i\sin\lambda\sigma_1 \end{bmatrix}, \tag{9}$$

which appears in Eq. (3.4) of Ref [11], can be simulated by choosing $U = \sigma_2$ and $V = \cos(\lambda/2)\sigma_2 + \sin(\lambda/2)\sigma_3$. By replacing this set of U and V in Fig. 3, a generalized quantum Fredkin gate is obtained. Details of other efficient quantum logic gate constructions will be reported elsewhere [14].

It would be interesting to know if the Fredkin gate can be built using fewer than six quantum two-body gates. If we only demand the output of a quantum Fredkin gate to be correct up to a phase, then Milburn [4] provides a three gate construction, but this is not a suitable building block for universal quantum computation. We believe that a construction of a true Fredkin gate using fewer than six quantum two-body gates, if possible, would have to involve a substantially different idea.

ACKNOWLEDGMENTS

This work is supported by DOE grant DE-FG02-90ER40542.

REFERENCES

[1] R. P. Feynman, Int. J. Theo. Phys. **21**, 467 (1982); D. Deutsch, Proc. Roy. Soc. Lond. A **400**, 97 (1985); D. Deutsch, Proc. Roy. Soc. Lond. A **425**, 73 (1989).

[2] R. P. Feynman, Found. Phys. **16**, 507 (1986).

[3] P. Shor, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.

[4] G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).

[5] P. L. Hagelstein, N. Margolus, and M. Biafore, preprint (1994); A. Ekert, preprint (1994).

[6] D. Deutsch, and R. Jozsa, Proc. Roy. Soc. Lond. A **439**, 554 (1992); E. Bernstein, and U. Vazirani, in *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing* (ACM, New York, 1993), p. 124; A. C. C. Yao, in *Proceedings on the 34th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1993), p. 352; D. R. Simon, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 116.

[7] C. H. Bennett, and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); C. H. Bennett, *et al.*, Phys. Rev. Lett. **70**, 1895 (1993); S. Popescu, quant-ph preprint # 9501020 (1995).

[8] R. Jozsa, and B. Schumacher, J. Mod. Optics **41**, 2343 (1994); Schumacher, Phys. Rev. A **51**, 2738 (1995).

[9] C. H. Bennett, IBM J. Res. Dev. **17**, 525 (1973); E. Fredkin, and T. Toffoli, Int. J. Theo. Phys. **21**, 219 (1982).

[10] T. Toffoli, in *Automata, Languages and Programming*, edited by J. W. de Bakker and J. can Leeuwen (Springer, New York, 1980), p. 632.

[11] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[12] D. P. DiVincenzo, and J. Smolin, in *Proceedings of the Workshop on Physics and Computation* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 14.

[13] D. Coppersmith, unpublished (1994); T. Sleator, and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[14] H. F. Chau, and F. Wilczek, in preparation (1995).

TABLES

Input			Output		
a_i	b_i	c_i	a_o	b_o	c_o
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

TABLE I. The “truth table” of a Fredkin gate.

FIGURES

FIG. 1. Fredkin gate, a_i, b_i, c_i are the inputs, while a_o, b_o, c_o are its outputs.

FIG. 2. (a) a quantum-NOT gate; (b) a conditional-U gate; and (c) a doubly-controlled phase shifter. We represent the control bit by drawing a dash line between its input and output.

FIG. 3. Construction of Fredkin gate using two one-body and seven two-body quantum gates.